Der schleichende Kontrollverlust über unsere privaten Informationen

von **Wolfgang Weller**

Einführung

Wir leben in einer Zeit ungeahnter und anscheinend auch unbegrenzter Möglichkeiten des Gebrauchs von Informationen und der Kommunikation. Diese Technologien bieten unbestreitbar vielerlei Nutzen und bereichern unser Dasein auf mannigfache Weise.

Spätestens seit der NSA-Affäre und den darauf folgenden Enthüllungen über das Ausspähen unserer Privatsphäre wird uns auch die dunkle Seite dieser Informationstechnologien vor Augen geführt. Inzwischen ahnt man, dass unsere persönlichen Daten, in einem bisher ungeahntem Maße und für uns weitgehend verdeckt, einem gigantischen Informationssystem zugeführt, dort gespeichert, auf geschickte Weise miteinander verknüpft und anschließend in einer für uns unkontrollierbaren Weise verwertet werden, deren Ergebnisse sich durchaus auch gegen uns Menschen wenden können. Dieser uns nicht zugängliche Verfügungsraum ist weitgehend ungeschützt. Es fehlt an Transparenz und auch jeglicher Möglichkeiten einer persönlichen Kontrolle. Damit sehen sich die Menschen ihrer Persönlichkeitsrechte beraubt. Kein Wunder also, dass die massenhafte Aggregation persönlicher Informationen und deren Verwendung für unkontrollierbare Zwecke bei vielen Menschen Ängste und Gefühle der Bedrohung auslösen. Dementsprechend wird ein besserer Schutz der Persönlichkeitsrechte angemahnt. Hier wird deutlich, dass Informationen ein überaus sensibles Gut sind, deren Besitz zu Macht und damit Einfluss verhilft. Die Kontrolle darüber möchte man nicht aus der Hand geben.

Während die Vorzüge und Nutzungsmöglichkeiten der modernen Informations- und Kommunikationstechnologie schon auf vielfältige Weise verdeutlicht und gewürdigt worden sind, sollen mit den nachfolgenden Ausführungen der weitgehend unbemerkten Gewinnung und Nutzung persönlicher Daten nachgegangen werden. Am Schluss werden wir noch auf Möglichkeiten zur Verbesserung des Schutzes verweisen.

1. Die vorliegende technologische Basis

Zunächst stellt sich die Frage, woher diese scheinbar aus dem Nichts kommende rapide Entwicklung der Informations- und Kommunikationstechnologie kommt. Die Antwort, so lässt sich sogleich sagen, liegt im Zusammentreffen verschiedener technologischer Faktoren.

Der dieser Entwicklung wird durch die durchgängige *Digitalisierung* der Informationswelt markiert. Damit ist es nunmehr möglich, Informationen jeglicher Art, seien diese sprachlicher, bildhafter, grafischer, biometrischer, orts- oder zeitbezogener Art, in einheitlicher Weise mittels Daten bzw. Datenströmen zu repräsentieren. Dies erlaubt eine einheitliche Handhabung von Informationen auch völlig unterschiedlicher Art und damit deren Speicherung und weitgehend beliebige Verknüpfung unter Verwendung von Computern. Damit eröffnen sich der Informationstechnologie völlig neue Horizonte.

Ein weiterer Meilenstein auf dem Weg zur modernen Informations- und Kommunikationstechnologie ist die verbreitete Einführung der *Funktechnologie*. Dafür wurde mit der Errichtung von Funknetzen eine flächendeckende Infrastruktur geschaffen, die eine fortlaufend gesteigerte Hochgeschwindigkeitsübertragung von Daten ermöglicht. Parallel dazu wurde eine völlig neue Art von *Endgeräten* für die Funkkommunikation auf den Markt gebracht. Aus den ursprünglichen Handys für einfache Sprachkommunikation entwickelten sich in kurzer Generationsfolge immer leistungsfähigere Geräte in Gestalt von iPhones, Smartphones, Tablet-PCs u. a., die eine komfortable Bedienung per Touchscreen bieten. Diese Endgeräte wurden durch Integration weiterer Informationsquellen, wie

Kamera und Navigationsempfänger, beständig aufgerüstet und hinsichtlich ihrer Funktionalität fortlaufend gesteigert. Einen weiteren Quantensprung bedeutete die Schaffung eines mobilen Internetanschlusses.

Dies alles zusammen hat innerhalb kürzester Zeit einer Entwicklung den Weg geebnet, welche wohl zu Recht als revolutionär bezeichnet werden kann und die auch zunehmend unser Dasein prägt. Damit bestehen nunmehr alle Voraussetzungen, um von jedem Ort aus und zu jeder Zeit via Funknetz zu kommunizieren und auch aus der Ferne gewisse Handlungen vorzunehmen. Parallel zu den Informationsleistungen, die über das Funknetz oder Bluetooth laufen, bietet das Surfen im Internet eine gewaltige Fülle zusätzlicher Dienstleistungen. Besonders bemerkenswert ist dabei die bestehende Möglichkeit, eine Vielzahl unserer Aktivitäten aus der Realität in die Sphäre der virtuellen Welt zu verlagern.

Neben all dem Nutzen der digitalisierten Informations- und Kommunikationstechnologie ist nicht zu übersehen, dass die Anhäufung gewaltiger Informationsmengen im Netz auch über uns selbst beträchtliche Risiken und Gefahren in sich birgt. Darin besteht die Kehrseite der Medaille, mit der wir zwar leben müssen, deren schädliche Auswirkungen wir aber möglichst stark begrenzen müssen.

Den nachfolgenden Ausführungen wird ein Denkmodell in Form eines weltumspannenden gigantischen Informationssystems unterlegt. Dieses System ist eigenaktiv, indem es, während wir es für unsere Zwecke nutzen, unerkannt persönliche Daten in anscheinend maßloser Fülle ablauscht, d. h. de facto unbemerkt kopiert und speichert. Der auf diese Weise gebildete Informationspool wird von verschiedenen Interessengruppen, zu denen auch die Geheimdienste gehören, umlagert, welche den Informationsbestand für eigene Zwecke nutzen. Dazu sind in das Informationssystem neben dem gigantischen Speicher auch Informationsverarbeitungseinrichtungen beträchtlicher Leistungsfähigkeit in Form verteilt angeordneter Computer integriert. Diese Rechner verarbeiten die vorliegenden Rohdaten unter Nutzung intelligenter Programme nach vorgegebenen Zielstellungen und speichern die Ergebnisse wiederum ab. Somit besteht ein gigantischer Datenpool, der aus verschiedenen Quellen fortlaufend angereichert wird. Bei der Verarbeitung werden die gespeicherten Rohdaten selbsttätig in einer für uns unkontrollierbaren Weise miteinander verknüpft, um aus den Ergebnissen bestimmte Schlüsse zu ziehen. Diese Ergebnisse werden den Menschen in einladender Form präsentiert, in der Absicht, sie damit in bestimmter Weise zu beeinflussen. Somit kommt es zu einem geschlossenen Informationskreislauf mit sehr komplexer Wirkstruktur. Manche nennen dieses System *Big Data*, weil dieses Gebilde vermeintlich alles über uns weis und unser Verhalten beeinflusst.

2. Wege zur Erfassung persönlicher Daten

Das im Zusammenhang mit der Funktechnologie und dem Internet entstandene weltweite Informationssystem enthält eine unüberschaubare Flut an Daten, deren Art und Zustandekommen wir zunächst untersuchen wollen. Hier lässt sich zunächst zwischen allgemeinen und persönlichen Daten unterscheiden.

Zu den *allgemeinen* Daten können wir Informationen von breitem Interesse zählen. Dazu gehören Informationen beispielsweise über das Wettergeschehen, bestehende Verkehrsverbindungen, den Sport, Reisemöglichkeiten, die Aktienkurse u. a. m., aber auch der Zugriff auf das in der virtuellen Enzyklopädie *wikipedia* hinterlegte lexikalische Wissen. Hier handelt es sich also vorwiegend um nützliches Wissen, das von kompetenter Seite und wissenschaftlichen Experten in das Netz gestellt wird und von dem wir auch selbstbestimmt Gebrauch machen.

Weitaus kritischer sind die *persönlichen* Daten. Diese gelangen auf unterschiedlichen und oftmals verschlungenen Wegen ins Netz. Wie sich schnell zeigt sind die Quellen, aus denen solche Daten geschöpft werden, durchaus vielfältig. Dementsprechend empfiehlt es sich, Unterscheidungen vorzunehmen.

Die unmittelbarste Art persönliche Daten ins Netz zu stellen besteht darin, dass dies von uns selbst und damit *freiwillig* geschieht. Die besonders bei Jugendlichen beliebten Einfallstore dafür sind die sog. sozialen Dienste, allen voran *Facebook* und *Twitter*. Obwohl auf diesen Kommunikationsplattformen zwischen den Partnern zumeist nur Belanglosigkeiten ausgetauscht werden, sind durchaus relevante Informationen darunter, welche sich nicht nur auf die Preisgabe des Standorts und Zeitpunkts der Kommunikation beziehen, sondern oftmals auch viel vom bildhaften Äußeren, den Eigenschaften, Gewohnheiten, Zielen und Wünschen der Teilnehmer verraten. An dieser Stelle kann schon mal Zurückhaltung bei der Preisgabe eigener Daten empfohlen werden.

Bedeutsamer indessen ist die *verdeckte Abschöpfung* persönlicher Daten, welche auf Grund unserer Aktivitäten im Netz produziert werden. Soweit wir uns dieser Netzdienste im alltäglichen Gebrauch bedienen, sind wir alle dieser Preisgabe ausgesetzt.

Je nach den genutzten Diensten kommen für die Absaugung persönlicher Daten unterschiedliche Quellen in Betracht. Dazu zählen das Abhören von Gesprächen, der Austausch von E-Mails, Finanztransaktionen mittels E-Banking, Warenkäufe über E-Commerce aber auch von uns eingegebene Suchanfragen beliebigen Inhalts. Das Ablauschen von Informationen erfolgt mittels verdeckt agierender Spähprogramme. Die auf diese Weise gewonnen Informationen verraten Vieles über uns, insbesondere unsere Tätigkeiten, Interessen, Gewohnheiten und Präferenzen. Diese Einblicke bieten vor allem den Großen ihrer Zunft, allen voran *Google* und *amazon,* hervorragende Möglichkeiten, sich ein Bild über uns Nutzer zu verschaffen. Aber allein schon die Sammlung einer möglichst großen Anzahl von E-Mail-Adressen bedeutet schon ein wertvolles Gut, da man diese für gutes Geld an durchaus vorhandene Interessenten verkaufen kann. Informationen haben also auch eine werthaltige Seite.

Eine andere ertragreiche Informationsquelle bietet auch das Mithören der funkbasierten Kommunikation über Handys. Neben den Inhalten sind allein schon Ort und Zeitpunkt der Gespräche von Interesse. Auch aus den Besuchen von Reisbüros, Tankstellen, Supermärkten, Restaurants und anderen Einrichtungen, bei denen zumeist mit der Karte bezahlt wird, können personenbezogene Daten bezogen werden. Es gibt auch durchaus Interessenten, die nach medizinischen Daten von Bürgern Ausschau halten. Solche lassen sich beispielsweise von Besuchen beim Hausarzt, den Aufenthalten in Krankenhäusern, beim Bezahlen von Medikamenten in Apotheken oder auch aus der Erfassung von Leistungen der Krankenkassen gewinnen.

Eine weitere abschöpfbare Informationsquelle beträchtlicher Ergiebigkeit sind unsere Automobile. Hier hat die beständige Aufrüstung unserer Fahrzeuge mit allerlei Automatisierungstechnik und insbesondere Assistenzsystemen zwar wesentliche Beiträge zur Verringerung der Umweltbelastung, allgemeinen Verkehrssicherheit und zum Personenschutz geleistet, bietet aber andererseits auch vielfältige Möglichkeiten zur verdeckten Abschöpfung persönlicher Informationen. So lassen sich bereits aus ganz normalen an Bord ermittelten Daten Informationen über bevorzugte Fahrgebiete, die tageszeitliche Nutzung oder Laufleistung des Kraftfahrzeuges gewinnen. Hier erweisen sich die Navigationsgeräte geradezu als Peilsender, deren orts- und zeitbezogene Daten viel über das Mobilitätsverhalten von Personen verraten. Das Verhalten von Fahrern kann wiederum anhand des Datenbestands von Brems-, Spurhalte- sowie Aufmerksamkeitsassistenten erkannt werden, indem die von der Automatik vorgenommenen automatischen Lenk- und Bremseingriffe oder ausgegebenen Warnhinweise ausgewertet werden. Die Möglichkeiten der Informationsgewinnung erweitern sich nochmals mit der von der EU-Kommission vorgeschlagenen Einführung des Notrufsystems *eCall (emergency call).* Weithin fortgeschritten ist auch die informationelle Fahrzeugvernetzung *Car_to_X_Communication.* Die Fahrzeuge kommunizieren dann in Echtzeit über eine von der Deutschen Telekom eigens dafür neuentwickelte funkbasierte Kommunikationsstruktur miteinander [3]. Eine überaus ergiebige Informationsquelle wird mit dem Ausbau von Automobilen zu Informationszentralen entstehen, welcher von den Automobilherstellern des Premium-Segments angestrebt wird [4]. Die PKWs dieser Sparte werden dann zu mobilen Datenbanken, die dann selbstverständlich auch über einen mobilen Internetanschluss verfügen [5]. Damit sind dann den Insassen auch während der Fahrt die Internetdienste

mit all ihren Möglichkeiten zugänglich. Zugleich bestehen aber auch die schon genannten Gefahren einer möglichen Abschöpfung persönlicher Daten.

Schließlich sei auch noch auf die auf Bahnstationen, neuralgischen Plätzen, Fußballstadien und anderen Begegnungsstätten mittlerweile übliche Überwachung durch festinstallierte Kameras verwiesen, über die massenhaft Bildinformationen mit der Zuordnung von Ort und Zeit in den großen Speicher gelangen. Dies erscheint einerseits im Sinne der allgemeinen Sicherheit als nützlich, birgt aber auch die Gefahr in sich, dass völlig unschuldige Personen fälschlich an den Pranger gestellt werden.

Die Liste der Möglichkeiten zur verdeckten Abschöpfung persönlicher Daten ließe sich leicht weiter fortsetzen. Allein die vorstehend genannten Beispiele der Gewinnung persönlicher Informationen verdeutlichen wohl hinreichend, dass aus völlig unterschiedlichen Quellen, unausgesetzt und für uns unbemerkt, persönliche Informationen erlangt werden, die sich unserer Kontrolle völlig entziehen.

Es erscheint notwendig, noch eine dritte Form der Datengewinnung zu erwähnen: das *Ausspähen*. Hierbei handelt es sich um das gewaltsame Eindringen in persönliche Datenbestände über das Internet. Hier versuchen unautorisierte und verdeckt arbeitende Personen in zumeist krimineller Absicht mithilfe eingeschleuster Trojaner oder Viren an Zugangsdaten unserer Computer, insbesondere unsere Bankverbindungen, Passwörter, PINs, TAN-Nummern und andere vertrauliche Daten heranzukommen. Bei dieser Ausspähung wird zumeist mit großem Geschick vorgegangen, so dass es unsererseits großer Aufmerksamkeit und auch wirksamer Schutzmaßnahmen bedarf, sich dagegen zur Wehr zu setzen.

3. Nutzungen des vorliegenden Datenmaterials

Es stellt sich naturgemäß die Frage, worin der *Sinn* einer solchen in der Summe gigantischen Datensammlung besteht, bzw. wofür dieses Datenmaterial eigentlich genutzt wird. Dies lässt sich wohl nur beantworten, wenn man die Ziele der daran Interessierten kennt. Auch hier sind durchaus Unterscheidungen zu treffen.

Eine erste und zugleich wesentliche Form der Datennutzung ist die *Identifikation* von Personen. Hier sind an erster Stelle die Geheimdienste zu nennen, welche die wohl umfassendste Erhebung und Auswertung persönlicher Daten betreiben. Das aus den verschiedensten Quellen massenhaft abgeschöpfte gewaltige Datenmaterial wird hier zur Fahndung nach bestimmten Personen ausgewertet. Dazu erfahren wir aus den Enthüllungen über diese Dienste, dass nicht nur bestimmte Zielgruppen, etwa Terrorverdächtige, in den Focus genommen werden, sondern die Daten prinzipiell *aller* erfassten Personen ausgewertet werden. Somit gilt wohl jeder als potenziell verdächtig. Aus dem Aufspüren terrorverdächtiger Personen schöpfen die Geheimdienste aus aller Welt, allen voran der US-amerikanische Dienst *NSA*, ihre Begründung für die Notwendigkeit einer umfassenden Ausspionierung praktisch der gesamten Bevölkerung. Das hier zugrunde liegende Prinzip der Identifikation besteht in der Ausfilterung von Personen aus einer übergroßen Gesamtheit von datentechnisch erfassten Menschen auf der Grundlage bestimmter Eigenschaftsmerkmale. Für die Bewältigung des gigantischen Datenmaterials kommen ausgetüftelte Filter- und Klassifikationsprogramme auf der Basis einer Eigenschaftsbeschreibung zum Einsatz.

Die *Identifikation* von Personen mag sicherlich bei der Fahndung nach Kriminellen und Terroristen hilfreich sein, ihre undifferenzierte und nicht hinreichend kontrollierte Anwendung kann aber, etwa bei fehlerhafter Personenbeschreibung oder Ermittlungsfehlern, auch völlig unschuldige Menschen an den Pranger stellen. Solche Personen fragen sich dann erstaunt, warum sie beispielsweise nicht in bestimmte Länder einreisen dürfen oder auch nicht mehr kreditwürdig sein sollen.

Aber auch unterhalb des Levels geheimdienstlicher Ermittlungen wird von unseren Daten gezielter Gebrauch gemacht, indem entweder nach Personen mit bestimmten Eigenschaften gesucht wird oder auch die Eigenschaften ausgewählter Personen erfragt werden. Hier macht man sich zunutze, dass durch

die vorangegangene Einstellung bzw. Abschöpfung persönlicher Daten im Netz mittlerweile so viel über die individuellen Eigenschaften von Personen bekannt ist, dass durch Zusammenführung dieser Informationen Personenbeschreibungen erstellt werden können. Diese digitalisierten Beschreibungen sind dann oft von ungeahnter Detailliertheit. Auf diese Weise gelingt es, Menschen als virtuelle Objekte zu repräsentieren. In diese Form gebracht, ist dann der virtuelle, und manche meinen auch „gläserne Mensch“, für ganz unterschiedliche Zwecke im Netz bestens verwendbar. Solche Dienste werden von sog. Big-Data-Firmen erbracht, welche sich mittlerweile im Internet tummeln.

Ein Beispiel ist die Verwendung von im Auto gesammelten Daten. Dazu lassen sich beispielsweise aus den während der Fahrt aus verschiedenen Quellen stammenden Daten Profile über die Fahrzeugnutzung und auch den Fahrer erstellen. Durch die Aggregation von immer mehr persönlichen Daten wird der Fahrzeugbenutzer allmählich zum „gläsernen Piloten“. An der Nutzung solcher Profile sind gewiss die Versicherer, Polizei, Logistikunternehmer und auch die Automobilindustrie interessiert.

Auch die aus verschiedenen Quellen abgeschöpften persönlichen Daten gesundheitsrelevanter Art können in geeigneter Weise miteinander verknüpft werden. Daraus werden dann Aussagen über die gesundheitliche Tauglichkeit von Personen erlangt. Dies dürfte nicht nur für Versicherer und Krankenhäuser, sondern auch für Personalchefs von Firmen von Interesse sein.

Aus der Zusammenführung von im Internet und dort insbesondere beim E-Banking und E-Commerce abgelauschten persönlichen Daten, können auch Fehleinschätzungen resultieren, die zu fatalen Folgen für die Betroffenen führen. Dementsprechend besteht durchaus die Gefahr, dass Banken oder auch die Schufa falsche Schlussfolgerungen bezüglich der Bonität oder Kreditwürdigkeit von Personen ziehen.

Eine andere Zielstellung für die Auswertung von Personendaten besteht in der *Vorhersage* menschlichen Verhaltens. Grundlage dafür ist insbesondere das Datenmaterial aus zuvor ermittelten Verhaltens- und Bewegungsmustern. Auch an dieser Möglichkeit sind die Geheimdienste wieder hochinteressiert. Das Ziel besteht hier in der rechtzeitigen Aufdeckung und damit Verhinderung vorbereiteter Terrorakte. Aus dem vorliegenden Datenmaterial wird unter Anwendung vor allem spieltheoretischer Methoden eine Prognose über die zu erwartende Tätigkeit von Personen erstellt.

Interessant sind Methoden der Verhaltensvorhersage aber auch für den Handel. Dort ist naturgemäß das Kaufverhalten der Kunden von Interesse, welches prognostiziert werden soll. Aus den ermittelten Erwartungen lassen sich dann Schlüsse ableiten, die etwa die Akzeptanz vorliegender Warenangebote, die Reaktion der Kundschaft auf Veränderungen der Warenpräsentation oder die Wirksamkeit von Werbemaßnahmen betreffen. Dieses Wissen ermöglicht wiederum eine Einflussnahme auf die Kaufgewohnheiten der Verbraucher. Bemühungen dieser Art reichen inzwischen bis hin zur *Manipulation* von Menschen. Hier wird nicht nur das Internet benutzt, sondern es werden im Grunde alle Medien in den Dienst gespannt, um Menschenströme zu lenken und vor allem den Warenabsatz zu steigern. An solchen Möglichkeiten sind vor allem die Warenhäuser und Marktketten jeder Art interessiert. Als wichtigstes Mittel zur Einflussnahme auf das Bevölkerungsverhalten gilt wiederum die gezielte Werbung (s. folgenden Abschnitt).

Eine weitere, jedoch recht unseriöse Verkaufstour aus der Rubrik der Einflussnahmen sind die in den Medien als kostenlos und zumeist mit großen Gewinnversprechen gepriesenen Kaffeefahrten. Mit solchen Verlockungen wird an die nicht unbedingt edelsten Eigenschaften von Menschen appelliert. Einmal leichtfertig ins Netz gegangen, entpuppen sich die versprochenen Vergünstigungen dann meist schnell als massive Nötigung zum Kauf überteuerter Ware.

Eine viel gefährlichere Form der Manipulation ist die Nutzung des Internets für Zwecke der Propaganda. Diese Plattform ist wegen ihrer Breitenwirksamkeit offenbar hervorragend geeignet zur Verbreitung schädlichen Gedankenguts und bietet damit Chancen zur *ideologischen Einflussnahme* auf breite Bevölkerungsschichten. Dieser Möglichkeit bedienen sich in durchaus geschickter Weise nicht nur Ideologen der rechte Szene, sondern auch Volksverhetzer und Hassprediger jeglicher Couleur. Der

Verbreitung solch gefährlichen Gedankengutes wird zwar, ähnlich wie bei den Pornos, durch gesetzliche Maßnahmen entgegengetreten, doch gibt es immer wieder Schlupflöcher.

An diese Stelle gehört noch der Hinweis auf die Verwendung erschlichener Daten für *kriminelle Zwecke.* Hier werden die Möglichkeiten des Informationssystems genutzt, um Personen oder auch Institutionen zuweilen beträchtlichen Schaden zuzufügen. Hier wird u. a. auf zumeist raffinierte Art versucht, an die eigentlich als geschützt geltenden persönlichen Zugangsdaten, wie Passwörter, ID-Codes zu gelangen oder auch Kontonummern auszuspähen, um auf unrechtmäßige Weise an Geld zu gelangen. Hier bedienen sich die Kriminellen oft raffinierter Tricks, vor denen man auf der Hut sein sollte.

Die Liste der Beispiele über die bestehenden Möglichkeiten eines unkontrollierbaren Gebrauchs unserer persönlichen Daten ließe sich leicht fortsetzen. Zusammenfassend müssen wir wohl feststellen, einer Entwicklung gegenüber zu stehen, bei der *Big Data* immer mehr Informationen über uns gewinnt und wohl auch Einfluss auf uns zu nehmen versucht. Die Befürchtungen, zunehmend zum „gläsernen Menschen“ zu werden, scheinen somit nicht unbegründet.

4. Die Überflutung mit unerwünschten Informationen

Die weltweit verfügbare vernetzte Informationstechnologie begünstigt nicht nur die flächendeckende Abschöpfung und Verwertung von Persönlichkeitsdaten für allerlei Zwecke, sondern eignet sich auch für eine nur schwer kontrollierbare *Überflutung* mit ungewollten und damit lästigen, nicht selten sogar schädlichen Informationen. An erster Stelle steht hier das uns in einem Übermaß zugehende Werbematerial für alle möglichen Produkte und Dienstleistungen. Kann man sich des den Zeitungen und Journalen in großen Mengen beigefügten Werbematerials noch auf einfache Art – nämlich durch Versenkung in die Altpapiertonne – entledigen, so ist der Umgang mit den uns täglich in einer Unzahl von E-Mails zuflatternden Werbungen schon problematischer. Diese unerwünschten Zusendungen knüpfen oftmals geschickt an im Menschen verankernde Instinkte an, indem oftmals große Gewinne oder die Aussicht auf Schnäppchen versprochen werden. Man entgeht diesen Versuchungen, oder zumindest Belästigungen, am besten durch Verwendung eines wirksamen Spam-Filters, welches uns vom Lesen solcher Mails abhält.

Überaus nervig mag man auch die im Fernsehen, besonders zu den Hauptsendezeiten in ununterbrochener Folge ausgestrahlten Werbespots empfinden, woran sich selbst die öffentlich-rechtlichen Sender beteiligen. In besonderer Weise betätigt sich hier die Pharmaindustrie mit dem Anpreisen ihrer Produkte, wobei jeder Spot endet mit dem nervigen Slogan: „Zu Risiken und Nebenwirkungen . . . “ – na ja, den Rest kennen Sie ja wohl bestens. Die Produktanbieter machen sich zunutze, dass die Zuschauer die nächste Nachrichten- oder Sportsendung nicht verpassen möchten und somit derlei Nötigungen kaum entgehen können. Und auch die Fernsehsender sind durchaus für Werbungen offen, werden solche Sendeclips doch gut bezahlt.

Weitaus gefährlicher sind indessen die äußerst geschickt verpackten Bemühungen mancher im Internet tätiger Dienstleister und Händler. Eine der besonders unangenehmen Formen ist das Verbreiten sog. *Spyware*. Hierbei handelt es sich um Spähprogramme bzw. Schnüffelsoftware, welche zumeist unbemerkt ihren Weg auf unsere Computer findet. Als gefährliches Einfallstor gilt besonders das Downloaden von als kostenlos gepriesenen Programmen. Passt man nicht höllisch auf, so werden die am Schluss der Offerte enthaltenen winzig kleinen Kästchen übersehen, welche vorsorglich schon mal mit einer Markierung belegt sind. Entgeht dies der Aufmerksamkeit des Benutzers, so werden nach dem Auslösen des Downloadbefehls zusammen mit dem gewünschten Programm ungewollt nicht nur weitere Werbeanzeigen, sondern – durchaus geschickt getarnt – auch unerwünschte und manchmal recht speicherintensive Programme mit heruntergeladen. Von diesen unerwünschten Cookies und Programmen wird der Rechner im Laufe der Zeit nicht nur regelrecht zugemüllt, sondern zusehens auch belastet, was sich wiederum in zunehmender Verringerung der Geschwindigkeit bemerkbar macht.

Diese Verlangsamung ruft dann wiederum ungewollt Anbieter von Schutz- und Sicherheitssoftware auf den Plan, welche – selbstverständlich wiederum kostenlos – heruntergeladen werden sollen. Hier besteht also ein echtes Minenfeld, in dem man sich nur mit äußerster Vorsicht bewegen sollte.

Insgesamt verbleibt ein Gefühl der teilweise recht aggressiv und manchmal bis an den Rand der Nötigung reichenden Bedrängung des Internetnutzers, was durchaus frustrierend sein kann.

5. Resultate

Die Ergebnisse der vorstehenden Untersuchungen lassen sich wie folgt zusammenfassen:

- Informationsabschöpfung und –verwertung

  Neben den von uns zuweilen leichtfertig in das Netz gestellten persönlichen Informationen wird ein offenbar erheblicher weiterer Teil davon in unterschiedlicher Weise und auf verdeckte Art gewonnen und in ein gigantisches Informationsnetz eingespeist. Dies erfolgt von uns weitgehend unbemerkt und ist daher auch nicht konzessioniert. Die extrahierte und im Netz abgespeicherte Menge an Rohdaten unterschiedlichster Art wird unter Nutzung immanenter Programme personenbezogen zusammengeführt und ergibt dabei virtuelle Abbilder von Personen. In anderen Fällen werden persönliche Profile erstellt, Bewegungsmuster ermittelt oder auch statistische Aussagen in Form von Verhaltenswahrscheinlichkeiten ermittelt. Für derlei automatische Datenaufbereitung kommen hocheffiziente Programme zum Einsatz, zu denen auch solche gehören, die sich auf die Spieltheorie gründen.

  Die Nutzung derart aufbereiteter Informationen erfolgt durch bestimmte Interessengruppen auf eine je nach Zielstellung unterschiedliche Weise. Als Hauptinteressenten gelten die Geheimdienste, Industriekonzerne, Geschäftswelt und möglicherweise auch die Politik. Dazu werden von diesen offenbar Dienstleistungen vergeben, indem Aufträge an Softwareagenten erteilt werden, welche diese wiederum selbstständig ausführen [1]. Die auf virtuellem Weg erlangten Ergebnisse können durchaus in realer Weise auf die betreffenden Personen zurückwirken. Beispiele sind neben der Entdeckung von Terroristen und die Verhinderung von Straftaten auch die erwartete Absatzsteigerung von Waren, Gewinnung von Geheiminformationen über laufende technische Entwicklungen bzw. Vorhaben etc. Ein Teil dieser Ergebnisse fließt wiederum auf informationellem Weg an die in den Focus genommenen Personen zurück. Dazu zählen etwa die Manipulation des Käuferverhaltens oder die ideologische Beeinflussung durch Propaganda. Durch die oftmals geschickte Art der versuchten Personenbeeinflussung werden die derlei Einflüssen ausgesetzten Menschen oftmals übertölpelt.

- Informationsüberflutung

  An die zuletzt beklagte informationell geführte Beeinflussung von Menschen anknüpfend muss noch auf die Informationsüberflutung eingegangen werden. Diesen unerwünschten und zumeist als belästigend empfundenen Darbietungen ist die Bevölkerungsmehrheit auf vielerlei Weise ausgesetzt. Besonders nervig und nicht selten gefährlich sind solche „Zuwendungen“ aber vor allem für die Internetnutzer. Es ist heutzutage keinesfalls mehr so, dass jemand, der sich Informationen über einen bestimmten Sachverhalt wünscht, nur diese selbst bestellt. Im Gegenteil werden die Menschen auf jede erdenkliche Art mit Informationen überschüttet, von denen die allermeisten uninteressant und unerwünscht sind. Einfallstore sind nicht nur die klassischen Medien, sondern besonders die Computer und Handys mit Internetanschluss. Der auf solche Arbeitsplattformen gelangte beständige Zustrom unerwünschter Informationen ist nicht nur nervig, sondern auch lästig, weil dieser die Arbeit behindert und Schutzmaßnahmen zur Eindämmung dieses Mülls erforderlich sind. Die ungebetenen Informationen werden aber

auch nicht selten zum Ausgangspunkt für Manipulationen oder gar einer Beraubung der angeschriebenen oder angemailten Personen.

Die vorstehenden Erkenntnisse führen zu dem Schluss, dass uns beim Umgang mit den neuen digitalisierten Medien die Selbstbestimmung und auch die Kontrolle unserer persönlichen Informationen vielfach aus der Hand genommen sind. Dies kann so weit gehen, dass wir irgendwo im Netz als virtuelle Personen landen, über die manchmal mehr bekannt ist als uns selbst bewusst ist. Und das Schlimme daran ist, dass wir damit auch den Gefahren fremder Einflüsse und Manipulationen ausgesetzt sind, deren wir uns nur schwer erwehren können. Dies verletzt nicht nur unsere Persönlichkeitsrechte, sondern ist auch in hohem Maß bedrückend.

Nun würde man annehmen, dass unsere Persönlichkeitsrechte ja durch das Grundgesetz geschützt sind. Wird – wie hier mehrfach erkannt wurde – dagegen verstoßen, so wäre dann wohl in erster Linie die Politik zuständig. Es wären dann wohl, zumindest strengere Regelungen und Gesetze zur Gestaltung und Begrenzung des Gebrauchs der digitalen Informationstechnologie notwendig. Von solch einem wirksamen Schutz der Bürgerrechte im Zeitalter von Internet, Funktechnologie, Smartphone und Computer ist jedoch derzeit noch wenig zu spüren. Über die Gründe dafür kann man nur Vermutungen anstellen.

6. Empfehlungen

Wenn die Schilderung des auf dem genannten Gebiet bestehenden Zustandes zutrifft, dann verbleiben nur ein eigenes besonnenes Handeln und die Inanspruchnahme verfügbarer Schutzmaßnahmen. Dazu sollen nachfolgend einige Hinweise gegeben werden (s. dazu auch [2]):

- Nimm Deine Eigenverantwortung wahr und stelle freiwillig so wenige Informationen von Dir ins Netz wie irgend möglich.
- Deinstalliere alle Programme, welche nicht unbedingt gebraucht werden.
- Verbanne wegen der bestehenden Sicherheitslücken möglichst Java-Programme, besonders aber Java-Script.
- Bei dem häufig benötigten Adobe Reader führe stets die angebotenen Updates durch, soweit diese seriösen Quellen entstammen.
- Soweit nicht bereits vorhanden, benutze ein leistungsfähiges Sicherheitsprogramm mit möglichst umfassendem Schutz und aktualisiere dieses periodisch unter Verwendung der angebotenen Updates.
- Misstraue jeder E-Mail, deren Absender Dir unbekannt ist. Beantworte solche nicht und komme auch keiner der dort genannten Handlungsaufforderungen nach.
- Lass Dich auch nicht durch das Verheißen von Gewinnen oder der Erlangung von Schnäppchen zum Öffnen von Mails bewegen.
- Benutze am besten einen Spam-Schutz, der Dir alle unerwünschten Mails fernhält.
- Gib auch auf Anforderungen niemals Passwörter oder ID´s von Dir preis.
- Benutze mehrere Passwörter von möglichst großer Länge und komplexer Struktur.
- Beim E-Banking halte das Überweisungslimit möglichst niedrig, um im Falle von Hackerangriffen den Schaden klein zu halten. Vertraue auch nicht allzu sehr auf den Schutz, den die Verwendung von TAN und iTAN versprechen.
- Beim E-Commerce leiste selbst auf Anforderungen niemals Vorauszahlungen.
- Kaufe lieber bei vertrauenswürdigen Anbietern als bei der billigsten Offerte zuzugreifen.
- Große Vorsicht ist bei Downloads geboten, da diese ein beträchtliches Gefahrenpotenzial enthalten können.
- Besondere Gefahren drohen bei kostenlosen Downloads. Schau Dir das Angebot genau an. Im unteren Teil sind häufig kleine Kästchen versteckt, die schon mal mit einer Markierung versehen

sind. Lösche unbedingt sämtliche Markierungen, bevor Du den Download-Button betätigst, andernfalls werden unerwünschte Spyware und viele unbrauchbare Zusatzprogramme mit heruntergeladen, was nicht nur nervig ist, sondern auch die Rechengeschwindigkeit vermindert.

- Benutze anstelle kostenloser Downloads wenn möglich lieber gekaufte Programme, dann bist Du auf der sicheren Seite.

Bei Beherzigung solcher und ähnlicher Ratschläge ist man schon mal ganz gut gerüstet beim Umgang mit dem *Big Brother* und seinen Trabanten.

Literatur:

[1] Weller, W.: Künstliche Agenten – eine Technologie mit großem Zukunftspotenzial. Druck und Verlag epubli GmbH, Berlin 2013, ISBN 978-3-8442-5642-0 (s. www.epubli.de)

[2] Rest, J.: Identitätsklau verhindern. Berliner Zeitung, Teil Wirtschaft, Nr. 22, 27. Jan. 2014, S. 10S

[3] N.N.: C2X „Soziales Netzwerk“ für Fahrzeuge. www.daimler-technicity.com, 15t. Aug. 2013

[4] Hänssler, B.: „Big Data“ auf der Straße. www.daimler-technicity.com, 29. Jan. 2014

[5] Brekeler, W.: Mobile Datenbank. Berliner Zeitung, Teil Mobile Welten, Nr. 33, 8./9. Jan. 2014, S. A1